IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

MARIA GREGORY and AYOMIPOSI ASAOLU, on behalf of themselves and all others similarly situated, Plaintiff, v. JOHNS HOPKINS UNIVERSITY and JOHNS HOPKINS HEALTH SYSTEM, Defendants.	**Case No. 1:23-cv-1854** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Maria Gregory and Ayomiposi Asaolu (collectively "Plaintiffs") bring this Class Action Complaint ("Complaint"), on behalf of themselves and all others similarly situated, against Johns Hopkins University and Johns Hopkins Health System (collectively "Hopkins" or "Defendants"), alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Entities that provide services in the healthcare industry and handle patients' sensitive, personally identifying information ("PII" or "Private Information") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of patients' PII to unauthorized persons—especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a breach of private data manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach

ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

3. As a major research university and healthcare service provider, Hopkins knowingly obtains sensitive patient PII and has a resulting duty to securely maintain such information in confidence.

4. Hopkins' Patient Privacy Policy and HIPAA Privacy Notice states that it uses "commercially reasonable security measures to protect the Personally Identifiable Information [Hopkins] collect[s] and store[s] from loss, misuse, destruction, or unauthorized access*"* and "The security of your information is important to us. We take precautions to protect your information by implementing safeguards to protect the information we collect."

5. As discussed in more detail below, Hopkins breached its duty to protect the sensitive PII entrusted to it and failed to abide by its own Privacy Policy. As such, Plaintiffs bring this Class action on behalf of themselves and the thousands of other employees, students and patients whose PII was accessed and exposed to unauthorized third parties during a data breach of Defendant's system on May 29, 2023, which Hopkins announced on or about June 14, 2023 (the "Data Breach").

6. Based on the public statements of Hopkins to date, a wide variety of PII was implicated in the breach, including but not limited to, patients' names, dates of birth, Social Security numbers and addresses.

7. As a direct and proximate result of Hopkins's inadequate data security, and its breach of its duty to handle PII with reasonable care, Plaintiffs' PII have been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

8. Plaintiffs are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their life. Consequently, Plaintiffs must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiffs, on behalf of themselves and others similarly situated, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

10. To recover from Hopkins for their sustained, ongoing, and future harms, Plaintiffs seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendants; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

Plaintiffs

11. Plaintiff Gregory is an adult who at all relevant times was a citizen of Severn Maryland residing in Anne Arundel County.

12. Plaintiff Gregory's PII was stored and handled by Hopkins. On or about June 30, 2023, Plaintiff Gregory was notified by Hopkins via letter dated June 23, 2023 of the data breach and of the impact to her PII.

13. Plaintiff Asaolu is an adult who at all relevant times was a citizen of Halethorpe Maryland residing in Baltimore County.

14. Plaintiff Asalou's PII was stored and handled by Hopkins. On or about June 30, 2023, Plaintiff Asaolu was notified by Hopkins via letter dated June 23, 2023 of the data breach and of the impact to his PII.

15. As a result of Defendant's conduct, Plaintiffs suffered actual damages including, without limitation, time related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. Plaintiffs and Class members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

Defendants

16. Defendant Johns Hopkins University is a private research university located in Baltimore, Maryland. The university's office is located at 3400 N. Charles Street, Baltimore, MD 21205.

17. Defendant Johns Hopkins Health System Corporation is a not for profit organization formed in 1986. The system's main office is located at 1800 Orleans Street, Baltimore, MD 21287.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' state of citizenship.

19. This Court has personal jurisdiction over the parties in this case. Defendant Hopkins conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b) because Hopkins and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

A. Hopkins and the Services it Provides.

21. The Johns Hopkins entity is structured as two corporations, the University and the Johns Hopkins Health System.

22. While administering services, Hopkins receives and handles PII, which may include, *inter alia*, customers' full name, address, date of birth, Social Security Number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

23. In order to receive services from Hopkins, Plaintiffs and the Class members are required to entrust their highly sensitive PII to Defendants. Plaintiffs and the Class members entrusted this information to Hopkins with the reasonable expectation and mutual understanding

that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. By obtaining, collecting, and storing Plaintiffs and the Class members' PII, Hopkins assumed legal and equitable duties and knew or should have known that Defendants were responsible for protecting Plaintiffs' and the Class members' PII from unauthorized disclosure.

25. And, upon information and belief, Defendants fund its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class members.

B. Hopkins Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Patients.

26. At all relevant times, Hopkins knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

27. On May 31, 2023, Defendants were notified by a third party vendor, MOVEit, that a data breach had occurred exposing Defendants' customers PII. Defendants performed an investigation and determined that an unauthorized third party had gained access to Defendants server that hosted the MOVEit software and was able to download sensitive information including Plaintiffs' and the Class members' PII.

28. Hopkins also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private health information.

29. These risks are not theoretical. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[1]

30. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[2]

31. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[3]

32. Further, a 2022 report released by IBM Security stated that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[4]

33. Indeed, cyberattacks against the healthcare industry have been common for over the past ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned

---

[1] *The healthcare industry is at risk*, SWIVELSECURE https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 17, 2023).

[2] *Id.*

[3] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[4] *Cost of a Data Breach Report 2022*, IBM SECURITY, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Apr. 17, 2023).

that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[5]

34. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[6]

35. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[7]

36. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

[5] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[6] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[7] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 17, 2023).

37. PII is a valuable property right.[8] The value of PII as a commodity is measurable.[9] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[10] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[11] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

38. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

39. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the

---

[8] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[9] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[10] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[11] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[12]

40. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

41. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites." [13]

42. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[12] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

[13] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

43. Based on the value of its patients' PII to cybercriminals and cybercriminals' propensity to target healthcare providers, Hopkins certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Hopkins Breached its Duty to Protect its Patients' PII.

44. On June 14, 2023, Hopkins posted a notice of "Data Attack" on its website that it experienced a security incident disrupting access to its systems.

45. As noted above, the patient PII compromised in the Data Breach includes demographic information and Social Security numbers.

46. Like Plaintiffs, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach.

47. All in all, approximately thousands of individuals with information stored on Hopkins's system had their PII breached.

48. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures in order to protect its customers' PII.

D. FTC Guidelines Prohibit Hopkins from Engaging in Unfair or Deceptive Acts or Practices.

49. Hopkins is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

50. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

51. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[15]

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[14] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[15] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[16] *Id.*

54. Hopkins failed to properly implement basic data security practices. Hopkins's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

55. Hopkins was at all times fully aware of its obligations to protect the PII of customers because of its position as an academic institution and healthcare provider, which gave it direct access to reams of customer PII. Defendants were also aware of the significant repercussions that would result from its failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

56. Cyberattacks and data breaches at healthcare companies like Hopkins are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

57. Researchers have found that among healthcare service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[17]

58. Researchers have further found that at healthcare service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[18]

[17] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[18] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RESEARCH 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

59. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

60. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

61. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

62. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit

[19] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[20]

63. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

64. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

65. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[21]

66. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-

[20] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

[21] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

marketing their products and services to the physical maladies of the data breach victims themselves.

67. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class members.

68. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

69. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [22]

[22] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).

70. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[23]

71. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[24] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[25] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

72. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

73. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against entities like Defendants is to get

---

[23] *Id.*

[24] *Id.*

[25] *Id.* at 4.

[26] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

74. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[27] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[28]

75. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[29]

76. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, an individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

[27] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[28] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[29] *Id.*

77. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[30]

78. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby making such information publicly available.

79. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [31] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[32]

80. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[33]

81. It is within this context that Plaintiffs and the Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

---

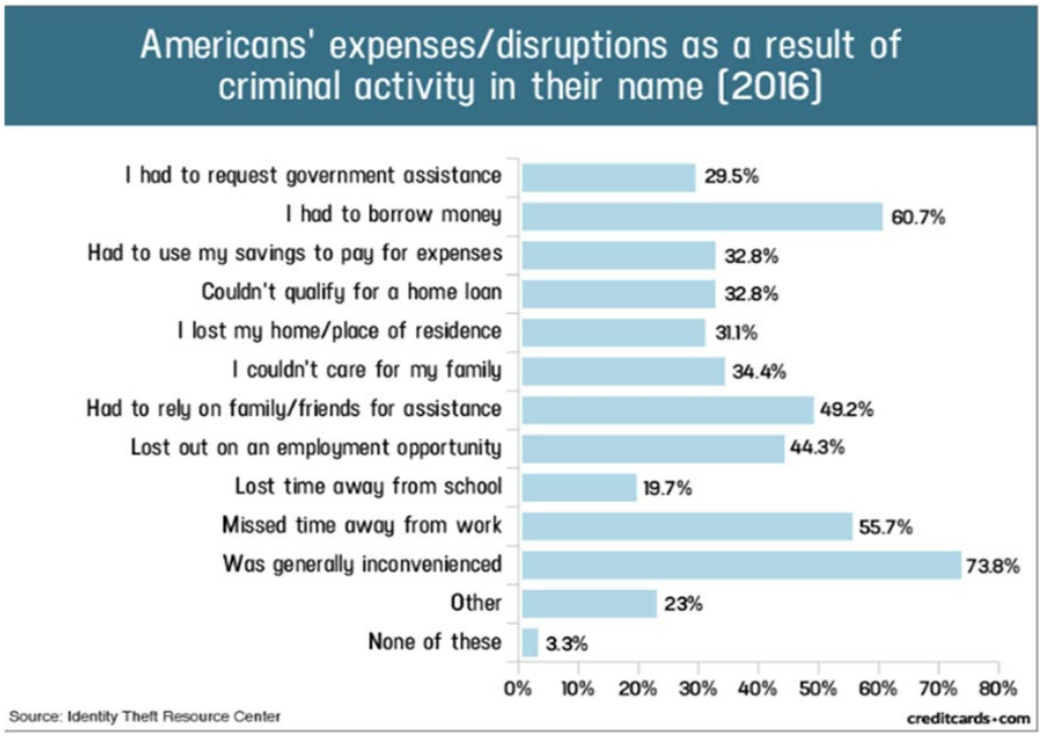
[30] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[31] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 17, 2023).

[32] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Apr. 17, 2023).

[33] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

82. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



83. Victims of the Data Breach, like Plaintiffs and the Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[34]

84. As a direct and proximate result of the Data Breach, Plaintiffs and the Class members have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing

[34] *Id.*

"freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

85. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which remains in the possession of Hopkins, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Hopkins has shown itself to be wholly incapable of protecting Plaintiffs' PII.

86. Plaintiffs and Class members also have an interest in ensuring that their personal information that was provided to Hopkins is removed from Hopkins's unencrypted files.

87. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Hopkins knew or should have known about these dangers and strengthened its data security accordingly. Hopkins was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

F. Plaintiffs Suffered Damages.

88. Hopkins received Plaintiffs' and Class members' PII in connection with providing educational and certain medical services and treatments to them. In requesting and maintaining Plaintiffs' PII for business purposes, Hopkins expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' and Class members' PII. Hopkins did not, however, take proper care of Plaintiffs' and Class members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Hopkins's inadequate security measures.

89. For the reasons mentioned above, Hopkins's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class members significant injuries and harm in several ways. Plaintiffs and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

90. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct.

91. Further, the value of Plaintiffs' and Class members' PII has been diminished by its exposure in the Data Breach. Plaintiffs and Class members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those described in their agreements with Hopkins for the benefit and protection of Plaintiffs and their respective PII. Plaintiffs and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

92. Plaintiffs and Class members would not have obtained services from Hopkins, or paid the amount they did to receive such, had they known that Hopkins would negligently fail to

adequately protect their PII. Indeed, Plaintiffs and Class members paid for services with the expectation that Hopkins would keep their PII secure and inaccessible from unauthorized parties. Plaintiffs and Class members would not have obtained services from Hopkins had they known that Defendants failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII from criminal theft and misuse.

93. As a result of Defendants' failures, Plaintiffs and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

94. Further, because Defendants delayed in notifying Plaintiffs and the Class members about the Data Breach for several weeks, Plaintiffs and the Class members were unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

95. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[35]

96. "Actors buying and selling PII from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's

[35] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Apr. 17, 2023).

utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[36]

97. Plaintiffs and the Class members are also at a continued risk because their information remains in Hopkins's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Hopkins fails to undertake the necessary and appropriate security and training measures to protect its patients' PII.

98. In addition, Plaintiffs and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

99. Plaintiffs bring all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons in the United States who had their Private Information submitted to Defendants or Defendant's affiliates and/or whose Private Information was compromised as a result of the data breach(es) by Hopkins on or about May 29, 2023, including all who received a Notice of the Data Breach (the "Class").

100. Excluded from the Class are Defendants, its subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

101. This proposed Class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the Class definition in an amended pleading or when they move

[36] David, *supra* note 67.

for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

102. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiffs are informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Hopkins's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes thousands of individuals.

103. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Hopkins failed to timely notify Plaintiffs of the Data Breach;

b. Whether Hopkins had a duty to protect the PII of Plaintiffs and Class members;

c. Whether Hopkins was negligent in collecting and storing Plaintiffs and Class members' PII, and breached its duties thereby;

d. Whether Defendant breached its fiduciary duty to Plaintiffs and the Class;

e. Whether Hopkins breached its duty of confidence to Plaintiffs and the Class;

f. Whether Hopkins violated its own Privacy Practices;

g. Whether Hopkins entered a contract implied in fact with Plaintiffs and the Class;

h. Whether Hopkins breached that contract by failing to adequately safeguard Plaintiffs and Class members' PII;

i. Whether Hopkins was unjustly enriched;

j. Whether Plaintiffs and Class members are entitled to damages as a result of Hopkins's wrongful conduct; and

k. Whether Plaintiffs and Class members are entitled to restitution as a result of Hopkins's wrongful conduct.

104. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class all had information stored in Hopkins's System, each having their PII exposed and/or accessed by an unauthorized third party.

105. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

106. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendants have acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

107. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent

a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Hopkins. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

108. Hopkins has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

109. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Hopkins failed to timely and adequately notify the public of the Data Breach;

b. Whether Hopkins owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Hopkins's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Hopkins's failure to institute adequate protective security measures amounted to negligence;

e. Whether Hopkins failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

110. Finally, all members of the proposed Class are readily ascertainable. Hopkins has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Hopkins.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiffs on behalf of the Class)

111. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

112. Plaintiffs bring this claim individually and on behalf of the Class.

113. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

114. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

115. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

116. Defendants' duty also arose from Defendants' position as a healthcare vendor. Defendants hold themselves out as a trusted provider of services for the healthcare industry, and thereby assumes a duty to reasonably protect patients' information.

117. Defendant breached the duties owed to Plaintiffs and Class members and thus was negligent. As a result of a successful attack directed towards Defendants that compromised Plaintiffs and Class members' PII, Defendants breached their duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

118. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their PII would not have been compromised.

119. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to

commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

120. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(Plaintiffs on behalf of the Class)

121. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

122. Plaintiffs bring this claim individually and on behalf of the Class.

123. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

124. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its patients.

125. Plaintiffs and members of the Class are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

126. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

127. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

128. As a direct and proximate result of Defendants' negligence, Plaintiffs have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(Plaintiffs on behalf of the Class)

129. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

130. Plaintiffs and Class members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

131. As a provider of electronic health record software, and recipient of patients' PII, Defendants have a fiduciary relationship to its patients, including Plaintiffs and the Class members.

132. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PII related to Plaintiffs and the Class. Plaintiffs and the Class were entitled to expect their information would remain confidential while in Defendants' possession.

133. Defendants owed a fiduciary duty under common law to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

134. As a result of the parties' fiduciary relationship, Defendants had an obligation to maintain the confidentiality of the information within Plaintiffs' and the Class members' medical records.

135. Defendants' patients, including Plaintiffs and Class members, have a privacy interest in personal medical matters, and Hopkins had a fiduciary duty not to disclose medical data concerning its patients.

136. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII of Plaintiffs and Class members, information not generally known.

137. Plaintiffs and Class members did not consent to nor authorize Defendants to release or disclose their PII to unknown criminal actors.

138. Defendants breached its fiduciary duties owed to Plaintiffs and Class members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

139. But for Defendants' wrongful breach of its fiduciary duties owed to Plaintiffs and Class members, their PII would not have been compromised.

140. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and the Class members.

141. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(Plaintiffs on behalf of the Class)

142. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

143. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

144. As a healthcare provider, Defendants have a special relationship to its patients, like Plaintiffs and the Class members.

145. Plaintiffs and the Class members provided Defendants with their personal and confidential PII under both the express and/or implied agreement of Defendants to limit the use and disclosure of such PII.

146. Defendants owed a duty to Plaintiffs to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

147. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII and confidential medical records of Plaintiffs and the Class members.

148. Plaintiffs' PII is not generally known to the public and is confidential by nature.

149. Plaintiffs did not consent to nor authorize Defendants to release or disclose their PII to an unknown criminal actor.

150. Defendants breached the duties of confidence it owed to Plaintiffs and Class members when Plaintiffs' PII were disclosed to unknown criminal hackers.

151. Defendants breached its duties of confidence by failing to safeguard Plaintiffs' PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c)

failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PII and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' PII and medical records/information to a criminal third party.

152. But for Defendants' wrongful breach of its duty of confidences owed to Plaintiffs and Class members, their privacy, confidences, and PII would not have been compromised.

153. As a direct and proximate result of Defendants' breach of Plaintiffs' confidences, Plaintiffs have suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendants – as a health care services provider – and Plaintiffs as a patient;

b. Theft of their PII;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII ;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual

and future consequences of the Hopkins' Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs and Class members' data; and

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendants.

154. Additionally, Defendants received payments from Plaintiffs and Class members for services with the understanding that Defendants would uphold its responsibilities to maintain the confidences of Plaintiffs' PII and private medical information.

155. Defendant breached the confidence of Plaintiffs and Class members when it made an unauthorized release and disclosure of their confidential PII and medical information and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiffs and Class members' expense.

156. As a direct and proximate result of Defendants' breach of its duty of confidences, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(Plaintiffs on behalf of the Class)

157. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

158. Plaintiffs had a reasonable expectation of privacy in the PII Defendants mishandled.

159. Defendants' conduct as alleged above intruded upon Plaintiffs' and Class members' seclusion under common law.

160. By intentionally failing to keep Plaintiffs and Class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiffs' and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class members' private affairs in a manner that identifies Plaintiffs and Class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class members.

161. Defendants knew that an ordinary person in Plaintiffs' or Class members' position would consider Defendants' intentional actions highly offensive and objectionable.

162. Defendants invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

163. Defendants intentionally concealed from and delayed reporting to Plaintiffs and Class members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

164. The conduct described above was at or directed at Plaintiffs and the Class members.

165. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

166. In failing to protect Plaintiffs' and Class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

167. As a direct and proximate result of Hopkins's conduct, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiffs on behalf of the Class)

168. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

169. Plaintiffs bring this claim individually and on behalf of the Class.

170. When Plaintiffs and members of the Class provided their PII to Hopkins in exchange for healthcare services, they entered into implied contracts with Defendants, under which Hopkins agreed to take reasonable steps to protect Plaintiffs' and Class members' PII, comply with it statutory and common law duties to protect Plaintiffs' PII, and to timely notify them in the event of a data breach.

171. Hopkins solicited and invited Plaintiffs and Class members to provide their PII as part of Defendants' provision of healthcare services. Plaintiffs accepted Defendants' offers and provided their PII to Defendants.

172. When entering into implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendants' data security practices complied with its statutory and common law duties to adequately protect Plaintiffs and Class members' PII and to timely notify them in the event of a data breach.

173. Hopkins's implied promise to safeguard patient PII is evidenced by, *e.g.*, the representations in Defendant's Notice of Privacy Practices set forth above.

174. Plaintiffs and Class members paid money to Defendants in order to receive services. Plaintiffs and Class members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Hopkins failed to do so.

175. Plaintiffs and the Class members would not have provided their PII to Hopkins had they known that Defendants would not safeguard their PII, as promised, or provide timely notice of a data breach.

176. Plaintiffs and Class members fully performed their obligations under their implied contracts with Hopkins.

177. Hopkins breached its implied contracts with Plaintiffs and Class members by failing to safeguard Plaintiffs' and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

178. The losses and damages Plaintiffs and the Class members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

179. As a direct and proximate result of Hopkins's breach of contract, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiffs on behalf of the Class)

180. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

181. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' Implied Contract claim.

182. Upon information and belief, Defendants fund its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class members.

183. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

184. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they purchased services from Defendants and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class members should have received from Defendants the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

185. Defendants knew that Plaintiffs and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiffs and Class members for business purposes.

186. In particular, Defendants enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase its own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security.

187. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members, because Defendants

failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

188. Defendants failed to secure Plaintiffs and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

189. Defendants acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

190. If Plaintiffs and Class members knew that Defendants had not reasonably secured their PII, they would not have agreed to provide their PII to Defendants.

191. Plaintiffs and Class members have no adequate remedy at law.

192. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and

identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

193. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

194. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class members overpaid for Defendants' services.

EIGHTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

195. Plaintiffs restate and reallege the preceding allegations the paragraphs above as if fully alleged herein.

196. Plaintiffs bring this claim individually and on behalf of the Class.

197. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

198. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

199. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

200. Defendants still possesses the PII of Plaintiffs and the Class.

201. Defendants have made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiffs' and Class members' PII.

202. To Plaintiffs' knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

203. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Hopkins. The risk of another such breach is real, immediate, and substantial.

204. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Hopkins, Plaintiffs and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

205. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Hopkins, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

206. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Hopkins implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Hopkins's systems on a periodic basis, and ordering Hopkins to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b. For equitable relief enjoining Hopkins from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Hopkins to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Hopkins's wrongful conduct;

e. Ordering Hopkins to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiffs on all claims so triable.

Dated: July 10, 2023

Respectfully submitted,

/s/ Andrea R. Gold
Andrea R. Gold (Bar No. 18656)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue NW, Suite 1010
Washington, DC 20006
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
agold@tzlegal.com

Marc H. Edelson (*pro hac vice* forthcoming)
Eric Lechtzin (*pro hac vice* forthcoming)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Telephone: (215) 867-2399
Facsimile: (267) 685-0676
elechtzin@edelson-law.com
medelson@edelson-law.com

Attorneys for Plaintiffs and the Putative Class